Counterterrorism in an Era of Competing Priorities

8 November 2019, Washington Institute for Near East Policy

Russell E. Travers
Acting Director, National Counterterrorism Center

What a pleasure to be here amongst so many old friends to share some thoughts on Counterterrorism in an Era of Competing priorities.

We are almost two decades removed from 9/11, and fortunately, we have been successful in preventing major attacks against the homeland. This success raises the important question of how counterterrorism should stack up against competing priorities, an increasingly relevant issue.

Ever since former Secretary Mattis issued the National Defense Strategy last year, there's been an ongoing conversation, at least implicitly, about risk. How does the threat of terrorism stack up relative to threats posed by great powers? Or North Korea? Or Iran? Or cyber?

I happened to have testified before Congress twice in the last two weeks, along with FBI and DHS leadership, to talk about threats to the homeland. Along with our discussion of terrorism, FBI and DHS leadership laid out a dizzying array of other threats to the homeland — election security, counterintelligence, intellectual property theft, and transnational organized crime — the last of which kills far more Americans than terrorism ever has, or ever will.

As I said at the two hearings, it is completely understandable that terrorism may no longer be viewed as the number one threat to the country. But what does that mean? I posed three questions for consideration:

- *What does the national risk equation look like as the Country confronts a very complex international security environment?*
- *How do we optimize our CT resources in the best interests of the Country when Departments and Agencies may have somewhat differing priorities?*
- *And if we're going to reduce efforts against terrorism how do we do so in a manner that doesn't inadvertently reverse gains of the past 18 years?*

For the next 35 minutes or so, I'd like to walk you through a bit of roadmap for the issues that I think need to be considered as we attempt to address those three questions. To do so, I'll be developing 10 themes, going from the geostrategic level to the electron level, and back up again.

THEME 1: Good News

Let me say at the outset that terrorism is not and never has been an existential threat to the Country, and will not be unless it changes who we are as a People. That said, it does hold out the potential for killing a lot of people, and as history has shown, it can occupy the Country's attention for a very long time, preventing other important things from getting done.

Fortunately, we've made a lot of progress on the terrorism front. For example:

- The last significant al Qaeda directed attack in the West was the Charlie Hebdo attack in Paris 5 years ago. The last centrally directed ISIS attack in the West was at a Turkish nightclub three years ago… and before that, Paris and Brussels.

- Homeland violent extremist (HVE) attacks are down, with only one in the U.S. this year and roughly ½ dozen in Europe. Both down substantially from previous years.

- While capabilities ebb and flow, we've seen ISIS struggle to sustain success, such as we've seen in Libya.

These successes have not been by accident. For example:

- There have been tremendous military and intelligence efforts in Iraq and Syria to eliminate the so-called Caliphate. As a result, many skilled operatives have been captured or killed, impacting terrorism resources, causing less sophisticated terrorist messaging, increasing terrorist infighting, and decreasing morale. These leadership removals have not been isolated to Iraq and Syria, but have taken place around the globe.

- The US government has pushed US borders further out, through screening processes and other efforts, to make the homeland less hospitable for terrorists.

- We've also seen global efforts to improve border security, particularly in the EU after the Paris and Brussels attacks.

- We've seen a growing partnership with the private sector to make cyber space less hospitable.

- And services around the globe are working together against terrorism unlike against any other national security threat.

- The U.S. government passes lessons learned to interested foreign partners with a robust exercise program to address information sharing and interagency cooperation.

- We are seeing capacity building in other countries, improvements in inter-service cooperation, and enhancements in information sharing that can mitigate the impact of terrorist attacks. For example, compare the Kenyan response to al-Shabaab attacks against the Westgate Mall in 2013 and Dusit hotel earlier this year. Kenya dealt with the latest attack faster and with fewer casualties than the prior attack.

We will never eliminate terrorism, but a tremendous amount of good work has been done, which facilitates a conversation about comparative risk.

THEME 2: A Concern for Complacency

Though we have had many successes, we need to be careful. When I started working counterterrorism after 9/11, we were overwhelmingly focused on al Qaeda and a centrally directed threat emanating from one piece of real estate along the Afghanistan/Pakistan border. 18 years later, we see a diverse, diffuse threat that spans the globe. For example:

- The primary Islamist threat in many of our countries is from homegrown violent extremists.
- Despite the elimination of the so called Caliphate, we have an active ISIS insurgency in Iraq and Syria and a sufficient command structure such that it maintains cohesion over twenty-odd ISIS branches and networks around the globe; some very small and others with thousands of people. As of today, nine groups have pledged allegiance to the new ISIS leader.
- We have al Qaeda, which has received rather less attention over the past few years than ISIS, but it too retains a command structure and ½ dozen affiliates, and we see growing connections and coordination between and among its affiliates.
- There remains a full range of Shia related threats, including Hezbollah and the Iranian Quds force as well as a growing concern for the Shia militant groups in Iraq.
- And if the various strands of Islamist extremism weren't complicated enough, we are also seeing a growing global threat of particularly extreme right wing-related terrorism, which I will discuss further in a moment.

Terrorists around the globe are proving very capable at exploiting technology. They're good at it. And they're innovative. We see this in:

- The use of encrypted communications for operational planning.
- The use of social media to spread propaganda and transfer knowledge between and amongst individuals and networks.
- The use of drones for swarm attacks, explosive delivery means and even assassination attempts.

- The use of high quality fraudulent travel documents that undermine a names based screening and vetting system and threaten border security.

- The use of crypto currencies to fund operations.

- And the potential terrorist use of chemical and biological weapons, which has moved from a low probability eventuality to something that is considered much more likely.

In many cases terrorist exploitation of technology has outpaced the associated legal and policy framework needed to deal with the threat. Looking out 5 years we are particularly concerned with the growing adverse impact encryption will have on our counterterrorism efforts. We can't freeze our thinking in 2019, but we must always be looking to the future.

Finally both al Qaeda and ISIS have shown themselves to be very successful at radicalizing vulnerable populations around the globe. We've seen these groups deploy emissaries to establish or organize a group or deploy an emissary to support an existing group if an emissary isn't already present with historic ties or personal connections. We've also seen groups deploy an emissary to ISIS core. We see radicalization done remotely via social media or letters or other very innovative ways that terrorists use to bolster their ranks.

THEME 3: Need for Focus on Prevention

The U.S. government is really good at going after terrorist leadership. As demonstrated a couple weeks ago, we can eventually find anyone on the planet. But ISIS and al Qaeda are movements as well as organizations and we can't capture and kill our way out of an ideology.

By any objective standard there are far more radicalized people now than there were on 9/11. Think tanks have suggested that we're looking at four times the number of radicalized individuals. And our own database of Known or Suspected Terrorists has grown by almost a factor of 20. So unless you believe the fervor will simply burn itself out, we will be faced with a growing radicalization problem around the globe.

No single factor captures the complexity of the radicalization process among disaffected Sunni youth worldwide. We believe a mix of **personal**, **group**, **community**, **sociopolitical**, and **ideological** factors contribute to radicalization, recruitment to extremist Sunni organizations, and mobilization to violence.

We are gradually accumulating more empirical data. For instance, the United Nation Development Program Regional Bureau for Africa evaluated 718 active or former African extremists — mostly from al-Shabaab or Boko Haram — to identify the reasons individuals were radicalized and recruited into extremist organizations. At the person level, the most important factor cited was human rights violations by the government security forces, but poverty, the nature of religious education, stable families, and government corruption were also cited.

But it's not just about poverty and being down trodden. As we saw in Sri Lanka, the individuals were well educated and relatively well off, but radicalized by hate preachers. There is a great deal of fertile ground in countries and we are facing growing radicalization in prisons and even amongst young children who are being targeted by extremist propaganda. There are various initiatives associated with messaging, deradicalization, defection programs, reintegration and off ramping around the globe — as well as broader programs focused on good governance, economic development and human rights. Available resources remains a significant global problem.

If the numbers of radicalized people around the globe keep growing, I don't like our odds of identifying the right people to capture or kill or to keep out of the Country. And there are second and third order effects. As the situation gets worse in Africa and climate change takes its toll, we are seeing greater forced migration. And the movement of migrants to Europe, in turn, is exacerbating tensions — giving further rise to right wing violence to protest this migration. It is a vicious cycle.

THEME 4: Need to Focus on Identities — People of Concern

Terrorist threats revolve around people and networks. And while tracking identities is pretty arcane, and not as interesting as talking about the future of ISIS or the latest strike, it is incredibly important. Our terrorist identities work underpins much of U.S. government screening and vetting architecture that evaluates 3.2 million people a day.

This is where we failed the Country on 9/11. Two of the hijackers were allowed to get visas, live in the Country and eventually get on airplanes because we were insufficiently stitched together. An enormous amount of effort has been expended over the past 18 years on this challenge. For example, we have effectively pushed borders out, creating a multilayered defense to identify individuals with terrorist connections at the earliest point. And we have continually improved: building richer dossiers, making better use of technology, performing near real time classified screening to support unclassified watchlists, and where possible, making use of biometrics.

This will never be a risk free proposition but the system has, overall, performed extraordinarily well. NCTC, working with our partners, is responsible for compiling the U.S. government database of KSTs – known or suspected terrorists – and our data is used to support our screening partners. There has been some confusion on this point, and when we talk about KSTs, precision is very important. Each day, approximately three individuals that meet the definition of KSTs seek entry or permission to come to the Country; this is not saying that they intend to conduct an attack — simply that there is sufficient derogatory information that warrants scrutiny. Upwards of another seven watchlisted individuals per day may have connections to KSTs, but we lack individual derogatory information required to consider them known or suspected terrorists.

As you might imagine, when three million people per day are screened, drawing conclusions about any one particular individual can be fraught with challenges, but over the course of 16 years the system has stood the test of time. In some cases, refugees for instance, extra levels of scrutiny are provided. We have no indication that foreign terrorist groups have attempted to exploit the refugee admissions

program, and robust screening and vetting probably limit their ability to do so. Over the past decade, there are only 2 individuals who arrived as refugees and went on to conduct attacks in the homeland; both radicalized after traveling to the U.S. The track record is pretty good.

However, as effective as we are at this, we can't sit on our laurels. And there are some warning signs.

As we saw in the Paris and Brussels attacks, many of the individuals were known to security services but had high quality fake passports or identification cards. Biographically based lists are on the wrong side of history. And we've already seen this in Northern Syria, where captured foreign fighters routinely gave fake names. Hence, FBI and DoD focus on biometrically enrolling people.

We've also got ever increasing amounts of information. How do we process all the volume of data and ensure high quality databases? I will go more into this later.

In my opinion we should be treating this period much like we did after 9/11. What are we trying to accomplish and how are we going to get there? We have a lot of pieces and parts and we need to ensure that they are stitched together.

The 5-10 year vision should be a near real time biographic and biometric screening against all available U.S. government information to determine if an individual is a KST. This would involve greater focus on collection, integration, and sharing of biometrics, as well as business process and IT architectural improvements. The benefits would extend well beyond counterterrorism and support screening against other categories of threats.

THEME 5: Need for Robust Intelligence:

None of this happens unless we maintain a robust integrated intelligence capability. There is no question that the CT Enterprise is the best integrated part of the Intelligence Community — we've been doing it as a Community for a very long time. But as good as we are, and as well-resourced, there will be significant challenges going forward.

A globally dispersed and diffuse terrorism threat that involves individuals and networks places great pressure on our Intelligence services. We need to evaluate the terrorist threat at multiple levels and have sufficient insight to determine if and when they pose a growing threat.

The first level is typified by the Sri Lanka problem. This was simply not a high priority before last Easter. The most hardline Islamist Group, Sri Lanka Thahweeth Jamath (SLTJ) had denounced ISIS in 2016. That spawned a much smaller entity, National Thahweeth Jamath (NTJ), that was apparently responsible. NTJ had been a bit of a fringe element primarily known for attacks on Buddhists statutes and not obviously associated with ISIS, so we didn't recognize the threat.

We are seeing local, indigenous Islamic insurgencies around the globe seek to affiliate themselves with ISIS. And with that comes greater interest in attacking western interests. Consider the long standing

insurgency in northern Mozambique, which is now affiliated with ISIS and focused on U.S. energy interests. Extrapolate that to the 20 current and budding ISIS affiliates around the world and you get some sense of the intelligence challenge.

Moreover, we need to have sufficient insight into these indigenous insurgencies to assess if or when they may be expanding beyond a local and regional threat to one that may threaten the homeland. This has been a challenge in the past:

- In 2009, we thought of AQAP as a regional threat, but on Christmas Day of 2009 Umar Farooq Abdulmutallab attempted to blow up NW Flight 253 over Detroit with an underwear bomb.

- And in 2010, we viewed the Pakistani Taliban as a regionally based South Asia threat. And yet they trained Faisal Shahzad who went on to attempt a bombing in NYC Time Square.

Think about the broad array of people and networks, and their ability to exploit technology. We have more than a few challenges:

- At the macro level as we adjust priorities to other threats, there is no question that intelligence resources — collection and analytic — will be shifted away from terrorism to other threat priorities. Actions have consequences. What do we stop focusing on? What is the associated risk?

- As we draw down military forces we will have less human intelligence and intelligence, surveillance, and reconnaissance capability in theater. There will be less liaison with on the ground partners. These are simply facts. With those facts comes a degree of risk, and we'll need to determine how great that risk is and whether it can be compensated for.

- And, then, at the national level we need to ensure that we have the right constellation of organizations and authorities. This is a large enterprise. There is duplication of effort. There will need to be rationalization going forward to ensure we are using resources wisely.

THEME 6: Need to Get the Electrons right

If we're going to get the intelligence right, we need to get the electrons right. Data is everything: whether looking for strategic trends, or conducting tactical level analysis associated with individuals and networks; data is the life blood of the CT community.

The data challenges we face are extraordinarily complex, particularly when we're dealing with information that is invariably incomplete, generally ambiguous, and often wrong. For example, 10 years ago this month, a Nigerian father walked into the Embassy in Abuja and said his son may be associated with extremists in Yemen. That cable was available to every CT analyst in the U.S. government — it got no attention, and a month later he tried to blow up NW Flight 253 over Detroit. Other data existed, but

the relationship wasn't obvious and we didn't connect the dots.

I've spent my entire career working analytic issues and will say unequivocally that counterterrorism has the worst signal to noise ratio of any discipline I've ever worked.

If I put you in the shoes of an NCTC analyst who has been working CT since 9/11, he or she has seen a quarter of million threats come across the screen; the overwhelming majority were bogus. But when they come in, how exactly do you know?

- To get a little more concrete we average about 300 threats to our embassies and consulates abroad every year — almost one a day.

- To get even a little more concrete, my ops center receives something in excess of 10,000 terrorism-related intelligence reports a day through which we need to sift. And those 10,000 reports contain 16,000 names. Daily.

All our services are challenged by the need to process ever expanding amounts of data in order to uncover potential terrorist plots. With the growth of captured media on the battlefield, or the explosion of social media, the magnitude of the problem only gets worse.

Terrorists have to communicate, move money, and travel, but strictly speaking these data sets aren't "terrorism information" so they can quickly implicate legal, policy, privacy and operational equities that limit the sharing and processing of such information. Determining which information is relevant, and addressing the competing equities associated with processing data remains a work in progress.

I will never have enough analysts to process the available information so Artificial Intelligence and Machine Learning are not "nice to have" they are an imperative. As such, I noted that earlier this week, the National Security Commission on Artificial Intelligence, chaired by Eric Schmidt, former Executive Chairman of Google, issued its interim report. Here's a quote from that report:

> "With respect to data, the government is well positioned to collect useful information from its worldwide network of sensors. But much of that data is unlabeled, hidden in various silos across disparate networks, or inaccessible to the government... Even more data is simply expelled as "exhaust" because it is not deemed to be immediately relevant."

And the infrastructure is woefully inadequate. We have a long way to go to realize the benefits of Artificial intelligence and machine learning.

In the case of terrorism, the problem is particularly difficult because so much of our data is unstructured. And it's all unstructured in different ways. That makes it very hard for machines to help us.

Hearken back to what I said about the evolving nature of the threat — it's all about individuals and networks. As we see with homeland violent extremists, it can be extraordinarily difficult to uncover

these individuals. The haystack has continued to grow and the needles are increasingly subtle; as such, prioritization becomes difficult. We are seeing this problem across the western world where partners may be dealing with thousands or tens of thousands of radicalized individuals and subjects of interest.

THEME 7: A rhetorical question: What does America want us to do in the realm of "discovery"?

Terrorism, like all transnational threats, poses unique challenges because it blurs concepts like "foreign" and "domestic." As such, our efforts to ensure public safety can quickly bump up against issues of privacy.

Part of the government's response after 9/11 was to provide NCTC with very broad authorities to receive terrorism information. In my opinion, that was a very good move. And with that came an extensive oversight and compliance regime and I'm extraordinarily proud of the Center's record in this regard. Indeed my experience has been that the entire Community is very conscientious about these issues.

But looking forward, and given the pace of technological change, it seems to me the issues are going to become more difficult and the need for an informed, transparent public discussion becomes greater. How do we square the circle — keeping the Country safe in a world of transnational threats that straddle the foreign and domestic divide, yet adequately balancing the protection of legitimate privacy rights? There's no consensus.

The notion of "**discovery**" is a case in point — linking non obvious relationships and finding "unknown unknowns" (so called "dot connecting"). How much can we, should we, do?

The processing of inexplicable amounts of information is enormously complex and defies any simple solution. International cyber criminals, terrorists, proliferators, and transnational criminals have linkages into the U.S. They may be U.S. persons with foreign connections. Or they may travel here, call here, or use our financial institutions. They use our openness against us.

Exploiting the attributes of globalization, terrorists can easily hide in the daily noise associated with millions of people that cross our borders... or the trillions of dollars that slosh around globally... or the unimaginable amounts of telecommunications activity. And in virtually all cases the data associated with these nefarious actors is sitting side by side in data repositories that also hold information on completely innocent U.S. persons.

There are a lot of complicated challenges that limit our ability to do discovery:

- In the case of the 12/25 "underwear bomber" it was a function of dots being lost in the background noise and an inability to discern non obvious relationships between two apparently innocuous pieces of information.

- In other cases, relevant data may exist in various Department and Agency repositories, but, for operational, law enforcement, or privacy reasons the information is not broadly available; retention and subsequent use issues are major limitations when it comes to co-mingling such information.

- And in still other cases, for instance in the case of financial data, the relevant information resides in entirely separate repositories that preclude large scale cross-stovepipe analysis.

Defaulting to slogans like the "need to balance privacy and security" may sound superficially attractive, but it isn't really helpful: which electrons should be accessible to which organizations, when, and for what purpose. Let me pose a few representative questions:

- First, what level and type of CT risk should we be willing to tolerate in order to preserve critical freedoms and liberties — and perhaps most importantly, how can the national security community structure a dialogue with the American public to constructively address this question?

- Second, how, as a national security community, do we govern and approach exploitation of the Internet, particularly at a time when (a) technology is far outpacing legal and policy rulemaking and (b) we're able to find information on the internet that is far more rich, valuable and intrusive than other types of collection subject to strict constitutional and statutory regulation?

- Third, what is the role of the private sector in national security and CT activities? Is there a point at which private sector and government are collaborating so closely — particularly in the area of data collection — that there is an intolerable privacy risk to individuals?

- I suspect these kinds of questions and the associated tradeoffs are going to be increasingly important as we look to the future.

Now, let me move away from electrons back to broader national security issues for the last three themes:

THEME 8: The Need for Whole of Government

Counterterrorism intelligence integration across all relevant departments and agencies, particularly in an era of constrained resources, will be both critical, and I suspect, increasingly difficult. It will also be insufficient. As we've found over the past two decades, we need "whole of government" integration — and that's always been a challenge.

As any practitioner will acknowledge, the reality of the way the Government is configured limits interagency effectiveness.

We are a Government of Departmental Sovereignty — the way we're designed, the way money is appropriated, and the way Congressional oversight works.

We have hard-wired silos of excellence across the Government. This is certainly not a new issue; endless studies have been written about the interagency process.

The 9/11 Commission had it about right: "It is hard to break down stovepipes where there are so many stoves that are legally and politically entitled to have cast-iron pipes of their own." But it is not impossible. One very good example was the post 9/11 watchlisting and screening architecture that brought together the entirety of the Government. But even that has been under stress as departments and agencies begin to adjust to evolving priorities.

NCTC's Directorate of Strategic Operational Planning has a role in convening the interagency to develop whole of government CT strategies. Arguably, the CT enterprise is more coordinated than any other mission, in part because of these efforts. That said, integration efforts such as these will always struggle in a system of departmental sovereignty and in the absence of sufficient authorities to compel cooperation.

Now in theory, integration happens at the National Security Council. It largely did in the years after 9/11 — CT was major focus at the most senior levels of the government because of the imminence of the threat. During a high-threat environment when we were routinely seeing major al Qaeda plots, tremendous interagency attention at all levels was devoted to terrorism. There were multiple Deputies and Principals Committee meetings every week.

Understandably, as the perceived threat declined, so did the degree of interagency focus. In addition there's been a degree of downsizing and deemphasizing National Security Council integration — a trend that goes back to the last Administration. There's been a sense that decisions could be kicked back to departments and agencies, partly because of a perception of "micro-management" and partly borne of a desire to wean departments and agencies off of relying on the NSC. We need to watch this very carefully to determine how well it does or doesn't work.

There's no question the NSC will continue to handle the very highest priority policy issues. But what happens when lesser important questions aren't recognized as important — until they are?

Remember, it was the very arcane subject of watchlisting and screening that failed the Country leading up to 9/11. And it was the technical issue of classified network access that gave rise to Wikileaks and eventually Snowden. How do we ensure lower visibility issues that implicate multiple department and agency equities get adequately addressed before they become strategic failures?

Finally, one result of a decline in NSC engagement is the potential for loss of interagency muscle memory. This could be incredibly important in the event of a need for a rapid response during crisis.

Terrorism, like any transnational threat, necessitates a Whole-of-Government response. As we move forward, we'll need to ensure that there are ample interagency mechanisms to effect such coordination.

THEME 9: The Need for Whole-of-Society

As we look to the future, we need to look beyond whole-of-government. Terrorist use of the internet will require a robust partnership between government and the technology industry to prevent the distribution of propaganda, communication with supporters, and proliferation of information to support attacks.

Over the past two years, there has been a marked increase in Industries' willingness to work with one another, the U.S. government and foreign partners to counter terrorism through the Global Internet Forum to Counter Terrorism (GIFCT). Originally created by Facebook, Microsoft, Twitter and YouTube, GIFCT provided a vehicle for discussions and potential information sharing.

There has been some substantial progress:

- Facebook, Twitter, and YouTube, have publicly reported that they detect over 90 percent of terrorist content through automated technology, meaning much of it is removed immediately after it is uploaded and never reaches the platform for public consumption.

- So far this year, YouTube has suspended over 42,000 channels and removed over 163,000 videos for promotion of terrorism; Facebook removed 6.4 million pieces of terrorist content in the first three months of this year; and Twitter suspended 166,000 unique accounts in the second half of last year for promotion of terrorism.

The recent move to establish GIFCT as an independent organization, or NGO, offers a more formalized opportunity to better leverage the respective strengths of the private sector and the U.S. government against this dynamic problem. The new construct looks to sustain and deepen industry collaboration and capacity, while incorporating the advice of key civil society and government stakeholders.

While it remains to be seen what role government entities will play within this construct, success against the future online terrorism threat will likely only be realized through greater transparency in information sharing across the public and private divide in near real-time.

Current transparency reports provided by the GIFCT members pertaining to their content take down efforts provide government entities with a snap shot of the scope and scale of the problem, but typically lack sufficient detail on the methods and the type of material that is being purged.

Government efforts to support technology companies could be better targeted with greater knowledge of the actual content being removed, the geolocation of its origin, and potential attribution. From this information, government entities would be able to more effectively assess trends in terrorist propaganda, identify new and emerging groups, key radicalizers, and credibility of potential plots. New insight could

then be passed back to the companies to enhance their models/algorithms.

None of this will be easy. Companies' willingness to more robustly engage governments depends on a host of policy, legal and proprietary concerns. But if we can mutually work through the impediments, there is no question that transparency would pay dividends.

Additional constructs might warrant consideration. I worked Transnational Organized Crime at the National Security Council and found Public/private partnerships like the National Cyber-Forensics & Training Alliance in Pittsburg to be a very useful platform. A 501(C)(3), the NCFTA brings together government and private sector representatives for the purposes of information sharing in the cybercrime arena; both government and the private sector have found the construct to be valuable.

As the threat evolves, we need to evolve. And that brings me to the last theme.

THEME 10: Getting our Arms around the global dimensions of Non Islamist Terrorism

Nothing highlights the evolving nature of the terrorist threat more than the growth of what some call DT. Others may call it "right wing" or "white supremacist" terrorism, and still others call it racially motivated violent extremism, or RMVE for short.

The FBI clearly has the lead on purely domestic terrorism. What I want to focus on here are global dimensions and the potential for a "movement."

The increasingly transnational nature of RMVE, facilitated by social media and online communication, has resulted in an environment that features frequent communication between sympathizers and an open exchange of ideas. A large percentage of RMVE attackers in recent years have either displayed outreach to likeminded individuals or groups, or referenced earlier attackers as sources of inspiration.

For instance, Anders Breivik, Dylan Roof, and Brenton Tarrant have gained international reverence and are serving as inspiration for many RMVEs, including those looking to plan or conduct attacks.

- Breivik has inspired—or at least been praised or researched by—at least five RMVE attackers or plotters since 2014, spanning from the U.S. to the UK, Germany and New Zealand.

- Roof has inspired at least two attackers or plotter since his June 2015 attack against a historic black church in Charleston, South Carolina.

- Tarrant—who himself was inspired by Breivik, and praised Roof, Bissonette, and other RMVE attackers—has inspired at least three attackers since his March 2019 attack in Christchurch, New Zealand.

The connections go beyond inspiration. We see overseas travel by white supremacists to fight in conflict areas, communications amongst racially motivated violent extremists, and the provision of funds. Some

of this involves connections to non-violent, but extreme "right wing" organizations. Some of this involves connections to active paramilitary groups or those that have been banned or designated as terrorist organizations by other countries, and some of this involves connections between like-minded individuals who might or might not someday move from exploring an extreme ideology to radicalization to mobilization to violence.

We don't fully understand how attackers are influenced and what constitutes meaningful relationships between extremists. Unlike Islamist extremism that in recent years has been led by relatively large and hierarchical organizations like al Qaeda and ISIS, RMVE does not feature authoritative or structured organizations or a monolithic ideology. Instead, it is dominated by lone attackers and small cells who use the online space as a borderless safe haven. They are inspired by a number of perceived concerns, including political, social, economic, legal, demographic, environmental and personal issues.

Moving forward, we will have to address a host of issues. Fortunately, there are lessons learned from our work in Islamist IT that could be applicable in the DT/RMVE space: whole-of-government, improved information sharing; a focus on individuals and facilitation networks; and working with the private sector and foreign partners.

That said, there are some challenges unique to this problem set:

- The lack of a DT Statute and associated materiel support charges,
- The added complexity of Constitutionally-protected free speech and the associated differences between the United States and our partners,
- And, the fact that perpetrators are often lone actors substantially complicates the kinds of designations used in IT.

But I'd also highlight two broader issues:

- First, for almost two decades the U.S. has pointed abroad at countries who are exporters of extreme Islamist ideology. We are now being seen as exporters of white supremacist ideology. That's a reality with which we are going to have to deal.
- Secondly, as we grapple with how to deal with a global RMVE movement, we need to be careful. In the case of the International Islamist terrorist threat, we lost some control of the narrative; amongst vulnerable Sunni populations radicalization has succeeded under the pretense that the west is conducting a war against Islam. False, but effective.

We need to guard against that in the RMVE space — we must disaggregate — appropriately dealing with violent white supremacist activity while not being perceived as painting with too broad a brush and impinging on legitimate right wing political activity and free speech.

Keeping control of the narrative and creating the international tool box for that particular disaggregation is going to be tricky, but absolutely necessary so as not to make the problem worse than it already is.

Conclusions

In conclusion, let me take you back to the questions I posed at the outset and on the Hill:

- What does the national risk equation look like as the Country confronts a very complex international security environment?

- How do we optimize our CT resources in the best interests of the Country when Departments and Agencies may have somewhat differing priorities?

- And if we're going to reduce efforts against terrorism how do we do so in a manner that doesn't inadvertently reverse the gains of the past 18 years?

Reasonable people could answer those questions in different ways. The answers are most assuredly not self-evident, and they deserve informed consideration by thought leaders inside and outside the government.

I do believe that the 10 themes I've laid out just now — that involve focusing on all aspects of the current and future terrorist threat, addressing a host of "must dos" and resolving a series of complicated, emotive issues — those themes will help us inform and develop a good government risk assessment as we move forward.

Thanks very much.